PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:
GEOFFREY S. STRONGIN
BRIAN C. BARNES
RODNEY SCHMIDT

Serial No.: 09/825,905

Filed: April 4, 2001

For: METHOD AND APPARATUS FOR SECURING PORTIONS OF MEMORY

Examiner: SHENG JEN TSAI

Group Art Unit: 2186

Attorney Docket: 2000.050200/TT3965

Customer No.: 23720

APPEAL BRIEF

CERTIFICATE OF MAILING UNDER 37 C.F.R. § 1.8	
DATE OF DEPOSIT:	5/2/06

I hereby certify that this paper or fee is being deposited with the United States Postal Service with sufficient postage as "FIRST CLASS MAIL" addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Signature

MAIL STOP APPEAL BRIEF - PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

On January 30, 2006, Appellants filed a Notice of Appeal in response to a Final Office Action dated October 4, 2005, issued in connection with the above-identified application. In support of the appeal, Appellants hereby submit this Appeal Brief to the Board of Patent Appeals and Interferences.

Since the Notice of Appeal for the present invention was received and stamped by the USPTO Mailroom on February 2, 2006, the two-month date for filing this Appeal Brief is April 2, 2006. A one month extension of time is hereby requested up to and including May 2, 2006 to timely file this response.

05/05/2006 SDENBOB1 00000065 09825905

01 FC:1401 500.00 OP
02 FC:1251 120.00 OP

An extension of time is required to enable this paper to be timely filed and there is no separate Petition for Extension of Time filed herewith, therefore, this paper is to be construed as also constituting a Petition for Extension of Time Under 37 CFR § 1.136(a) for a period of time sufficient to enable this document to be timely filed.

A check in the amount of $500.00 is enclosed for the filing fee of this Appeal Brief. In addition, a second check is enclosed in the amount of $120.00 for the extension fee of one month. No other fee is believed to be due in connection with the filing of this document. However, should any fee under 37 C.F.R. §§ 1.16 to 1.21 be deemed necessary for any reason relating to this document, the Commissioner is hereby authorized to deduct said fee from Williams, Morgan & Amerson, P.C., Deposit Account No. 50-0876/2000.050200/TT3965.

I. REAL PARTY IN INTEREST

The present application is owned by Advanced Micro Devices, Inc.

II. RELATED APPEALS AND INTERFERENCES

Appellants are not aware of any related appeals and/or interferences that might affect the outcome of this proceeding.

III. STATUS OF CLAIMS

Claims 1-24 remain pending in this application.

The Examiner rejected claims 1-4, 7-9, 11-13, 15-17, 19-21 and 24 under 35 U.S.C. 102(b) as being anticipated by ***Nozue*** (U.S. Patent 5,890,189), and rejected claims 5-6, 10, 14, 18, and 22-23 over ***Nozue*** and in view of ***Childs*** (U.S. Patent 4,442,484).

The claims currently under consideration, *i.e.*, claims 1-24, are listed in the Claims Appendix submitted herewith.

IV. STATUS OF AMENDMENTS

After the Final Rejection, no other amendments were made to any other claims.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The Examiner rejects independent claims 1, 19, and 24 over Nozue. These claims are generally directed at providing at least two layers of protection for information stored in a memory. The information sought to be protected is referred to as "selected information" in the claims. As described in the patent application, some systems provide protection using page or segment tables. *See* Patent Application, page 3. But, also as noted in the patent application, this type of arrangement may not be adequate for protection. *See Id.* at 15-21. The specification describes an embodiment in which another table (*e.g.,* shown in Figure 5) that associates at least one of read and write privilege with one or more physical addresses of a memory that houses the selected information. In sum, the patent application describes controlling access to selected information using attributes defined in a first table (such as a segment or page table for example), and second table that associates read and/or write privilege with the physical addresses of the memory. In this manner, the selected information can be securely protected. For example, the patent application states that by "controlling access at the physical level" (through the use of the

second table), it is "difficult for programs to gain unauthorized access by first mapping virtual pages to the protected memory location and then indicating in the alias page table entry that the protected memory is write enabled," *Id.* at p.18, lines 13-16. The claims 1, 19, and 24 are directed to one or more features of the embodiments described in the specification.

Claims 11 and 15 (and their respective dependent claims) similarly provide two-levels of security for controlling access to select information. Claim 7 and its dependent claims are directed to an embodiment for controlling access to information through the use of a first and second security levels. Additional details describing the various aspects of disclosed embodiments can be found in the patent application.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1. Whether claims 1-4, 19-21 and 23-24 are anticipated by ***Nozue***?

2. Whether claims 11-13 and 15-17 are anticipated by ***Nozue***?

3. Whether claims 7-9 are anticipated by ***Nozue***?

4. Whether claims 5, 10, 14, 18, 22 and 23 are patentable over ***Nozue*** and in view of ***Childs***?

5. Whether claim 6 is patentable over ***Nozue*** and in view of ***Childs***?

VI. ARGUMENT

The Examiner's rejections in the instant case have been based on generalities. When pressed during prosecution to provide more details, the Examiner largely failed to respond with any meaningful level of specificity. In the few instances that the Examiner did elaborate on the

rejections (mainly in the Advisory Action), the Applicants have fully addressed those arguments in this brief. The Applicants also note other deficiencies in the Examiner's rejections in this brief. In view of the inadequacies in the Examiner's rejections, the Applicants fully anticipate that the Examiner will likely raise new theories of rejection (based on the same references) in his Answer to compensate for the existing flaws in order to make a prima facie case of anticipation and obviousness. The Applicants respectfully reserve their right to address any new theories that the Examiner may raise in the Answer.

The pending claims are allowable for Nozue and/or Childs for reasons set forth more fully below.

A. Claims 1-4, 19-21 and 23-24 are not anticipated by *Nozue*

Claim 1, which is representative of other claims in this section, is discussed first. Claim 1 calls for a method for providing security in a computer system. The method includes controlling access to selected information using attributes defined in a first table. The method further calls for controlling access to the selected information using a second table that associates at least one of a read and write privilege with one or more physical addresses of a memory that houses the selected information. As is evident, the term "selected information" in the second claim element derives its antecedent basis for the first claim element. Thus, reading the first two claim elements together, claim 1 provides that both the first and second tables operate to control access to the same selected information.

The Examiner asserts that Nozue teaches all of the features of claim 1. The Applicants respectfully disagree and assert that Nozue at least fails to teach (1) a second table that associates at least one of a read and write privilege with one or more physical addresses of a memory and (2) controlling access to the selected information using two tables. Each of these deficiencies in Nozue is discussed in detail below.

In rejecting claim 1, the Examiner asserts that the first table of claim 1 corresponds to the table shown in Figure 45 of Nozue, and the second table corresponds to the table shown in 24A of Nozue. See Final Office Action, page 4. The Examiner further argues that table 24A shows associating read/write privilege(s) with physical addresses of a memory (as called for by claim 1) because it illustrates the association of "logical address (311), **a physical address (312)**, and the read/write/execution (rwx, 323) privilege". *see* Advisory Action, p. 2 (emphasis added). The Applicants respectfully disagree because Nozue describes association with "physical page numbers," whereas the claim calls for association with "physical address of a memory." In the instant case, the Examiner mischaracterizes the Nozue reference. Element 312 of Figure 24A is not a "physical address of a memory" (as the Examiner contends), but rather the "physical page number." One need not look any further than Figure 24A itself to understand that that element 312 is labeled as "PHYSICAL **PAGE NO.**" (emphasis added). Indeed, the specification confirms this understanding when it states that each entry includes a physical page number 312. Nozue, 24:60-63.

To the extent that the Examiner is arguing that a "physical memory address" is the same as a "physical page number," the Examiner's argument is squarely undercut by the teachings of

Nozue. Nozue itself distinguishes between the two terms and uses them to refer to different things. In particular, Nozue clarifies that the "physical page numbers" themselves are not the physical memory addresses but rather they are page numbers that are *defined* by physical memory addresses. *See* Nozue, 23:58-63 (describing that a memory management unit operates to *obtain* a physical page number *defined* by the physical memory address) (emphasis added). Similarly, other portions of Nozue further clarify that "physical page number" (shown in Figure 24A) is different from the claimed "physical address of a memory." *See* Nozue, 24:41-46 (describing the "*physical addresses corresponding* to this *physical page number* in...the TLB") (emphasis added).

To show anticipation, the Examiner must show that that the cited reference teaches each claim element identically. Here, the Examiner has at least failed to show a second table that associates at least one of a read and write privilege with one or more physical addresses of a memory. For this reason alone, claim 1 and its dependent claims are allowable. Moreover, claims 19-21 and 24 are also allowable for this reason.

Even assuming *arugendo* that that the "physical page number" corresponds to the "physical address of a memory," Nozue still does not teach or disclose associating a read or write privilege with the physical address (or "physical page number"). Nozue describes that the "rwx" permission bits 323 in Figure 24A are associated with each of the threads 318. Nozue, 25:5-6 (stating that "memory access mode permission (*rwx*) 323 [are] *associated with* each of the *thread* numbers 318") (emphasis supplied). In contrast, claim 1 calls for associating the read/write privilege(s) with the physical address of the memory (as opposed to threads).

The Examiner contends that Figure 24A shows physical page number field 312 being associated with the rwx bits 323. *See* Advisory Action, page 2. The Examiner's argument is misleading. In Figure 24A, the depicted physical page number 312 corresponds to each logical page number 311. *See* Nozue, 24:62-63 (stating that the "physical page number 312 correspond[s] to the logical page number 311"). The permission "rwx" bits, on the other hand, are associated with the threads (as discussed above), and not with the physical page numbers. Nozue describes that these permission bits determine whether a particular thread can access (read/write/execute) the logical page number 311 (or the corresponding physical page number 319). *See* Nozue, 25:28-32 (stating that the permission mode (rwx) 323 indicates whether the logical page in the TBL is readable, writable, and executable by the thread 318). This is consistent with Figure 24A, which shows that each thread 218 has associated permission (rwx) rights for a given logical page 311 (or corresponding physical page 319).

Indeed Figure 24A illustrates that, for any given logical page 311 (or its corresponding physical page 319), different threads can have different access permissions. For example, one thread 318 may have only write access to the logical/physical page, while another thread 318 may have only read access to that same page. Because a given page can have different access permissions (depending on the rights assigned to the threads), this point reinforces the Applicants' point that the access permissions in Nozue flow with the threads, and not the logical/physical page. In contrast, as claimed and as shown in Figure 5 of the patent application, the access rights are associated with memory addresses (or locations), where, for example, each location has its own "read only" or "write only" access. Because the access permissions in

Nozue are associated with threads, and not physical address of the memory, claim 1 (and the other claims in this section) is allowable for at least this additional reason.

Claim 1 (as well as the other claims in this section) is also allowable because Nozue does not teach controlling access to the "selected information" using two tables. In the first two Office Actions, the Examiner continually failed to identify with any meaningful level of specificity as to what in Nozue corresponds to "selected information." It is only in the Advisory Action, after the Applicants highlighted this deficiency in the Examiner's rejection, that the Examiner finally revealed his position – namely, the Examiner noted that the "contents of the first and the second tables correspond to the 'selected information'." (emphasis added). For the purposes of this appeal, the Applicants address the Examiner's rejections based on the Examiner's assertion that the "selected information" corresponds to the contents of the two tables described in Figure 45 and 24A.

The table of Figure 45 of Nozue shows a program management table, and Nozue describes that it is used to track the logical address space of a program that is mapped to the same logical address space as other programs. Nozue, 42:6-8; 41:47-53. In contrast to table 45, Figure 24A of Nozue illustrates a translation look-aside buffer (TLB) that includes a plurality of entries, where each entry includes a logical page number of a thread, a corresponding physical page number of the logical page number, and access permissions for each thread. To show anticipation under the Examiner's application of Nozue (where the "selected information" corresponds to the "contents" of theses tables), the Examiner must show that both tables "control access" to each other's contents. However, this is clearly not the case. As can be seen, the two

tables in Nozue serve two independent, different purposes – Figure 45 table tracks logical address space for programs mapped to a common logical address space, whereas Figure 24A is a translation look-aside table that defines access permissions for various threads. As such, neither table "controls access" to the "contents" of the other table. In contrast, as noted, claim 1 calls for controlling access to the same selected information using two tables. For this additional reason, claim 1 (and the other claims in the section) is allowable.

B. Claims 11-13 and 15-17 are not anticipated by *Nozue*

Claims 11-13 and 15-17 are also allowable over Nozue. Claim 11 is discussed first. Among other things, claim 11 calls for (1) protecting selected information using a first level of security specifying access privileges to the selected information and (2) protecting the information using a second level of security that associates at least one of a read and write privilege with one or more physical addresses of a memory that houses the selected information. Claim 11 thus calls for two-levels of providing security.

The Examiner's rejection of claim 11 is deficient for the same or similar reasons as it is deficient with respect to claim 1. For example, for reasons set forth above, Nozue at least fails to teach associating at least one of a read and write privilege with one or more physical addresses of a memory. Additionally, Nozue does not teach protecting the selected information using two levels (as the first and second levels are specified in the claim), much like Nozue does not teach controlling access to the "selected information" using two tables in claim 1. Thus, the arguments

stated above with respect to claim 1 apply to the claims in this section, wherever appropriate. For at least these reasons, claim 11 (and other claims in this section) is allowable.

C. Claims 7-9 are not anticipated by *Nozue*

Claims 7-9 are also allowable of Nozue. Claim 7, which is representative of the other claims, calls for writing to at least one register to define a privileged memory region. Claim 7 further specifies defining at least one computer instruction as a privileged instruction, wherein the privileged instruction is resident in the privileged memory region. Thus, reading the second claim feature in light of the first feature, claim 7 calls for storing the privileged instruction in the memory region, where that memory region is defined by the at least one register (see the first feature of claim 7).

Claim 7 further calls for (1) identifying information for protection and (2) indicating at least one physical address of a memory that houses the information as at least one of read and write disabled. Thus, when these two features are read together, claim 7 calls for indicating the physical address of the memory that houses the information sought to be protected as read and/or write disabled.

Finally, the last element of claim 7 calls for controlling the access to the information using the privileged instruction. The "privileged instruction" referenced here is that same instruction which is resident in the privileged memory region (see first and second elements of

claim 7). The last element thus specifies controlling access to the information that is housed in the memory that is marked as read/write disabled using the privileged instruction.

The Examiner asserts all of the elements of claim 7 are disclosed by Nozue. The Applicants disagree. The Examiner argues that the "at least one register" of claim 7 that defines the claimed "privileged memory region" is shown as element 17 of Figure 3 of Nozue. *See* Final Office Action, p. 6. Element 17 of Figure 3 is referred to as a "current memory protection information" in Nozue, and is used to store a memory protection information for the currently executed instruction. Nozue, col. 7, lines 44-47. In particular, Nozue describes that element 17 includes a current transition permission 4, a current execution permission 5, and a current right permission 6 for the current executed instruction. *Id.* Thus, Nozue describes that the current memory protection information 17 stores various permissions (e.g., transition permission, execution permission, right permission) of the currently executed instruction. In contrast, claim 7 calls for writing to at least one register to define a privileged memory region in which the privileged instruction is resident. Accordingly, for this reason alone, claim 7 and its dependent claims are allowable.

The Examiner erroneously argues that Nozue also discloses the third element of "identifying information for protection." With respect to this feature, the Examiner argues that the "information" identified for protection corresponds to "instruction" 14 and "data" 15 in Figure 3 of Nozue. *See* Final Office Action, p. 6. Items 14 and 15, however, are signal generators, as shown in Figure 3. They are not "information," as called for by claim 7. The Examiner's flawed position on this point is further exposed when it is considered in view of the

next claim element, which calls for indicating at least one physical address of a memory that houses the information as at least one of read and write disabled. In this element, the term "information" derives its antecedent basis from the earlier claim element. As such, the term "information" refers back to the previous mention of "information" (which the Examiner asserts correspond to signal generators 14, 15). In Nozue, the signal generators 14, 15 are not "housed" in any memory but rather are devices (as the name implies) that generate signals. Because the generators 14, 15 ("information" according to the Examiner) are not stored in any memory, it follows that no physical address of a memory can be indicated as read and/or write disabled, as called for by claim 7. For at least the following reasons, claim 7 (and other claims in this section) is allowable.

Response to Examiner's Argument

In the Advisory Action, the Examiner changed his argument from the Final Office Action, and asserted that element 3 (as opposed to the originally identified element 17) in Figure 3 "defines a memory region in which the privileged (i.e., protected) instruction is resident." *See* Advisory Action, page 2. The Examiner's new theory, however, is equally deficient as the original one, as explained below.

In Nozue, element 3 is a "current segment identifier" that identifies a segment in which a currently executed instruction is present.[1] *See* Nozue, 13:41-50. Because claim 7 calls for the

[1] Indeed, this fact is also recognized by the Examiner. *See* Advisory Action, page 2.

"privileged instruction" to be resident in the "privileged region," the Examiner must demonstrate that the "segment" identified by element 3 contains the "privileged instruction." If that were not the case, then the "privileged instruction" would not be "resident" in the region defined by the register, as called for by claim 7. In the instant case, as noted, the only instruction present in the "segment" is the "currently executed instruction." But this instruction cannot be the claimed "privileged instruction" because claim 7 specifies that the "privileged instruction" is used to "control access" (see last element of claim 7) to the information stored in the memory. Here, it is helpful to recall, that the claimed "information" according to the Examiner corresponds to the signal generators 14, 15 in Nozue. In Nozue, the "currently executed instruction," however, does not control access to the information ("signal generators 14, 15"). Because the Examiner has failed to specifically point to anything in Nozue that discloses that the "currently executed instruction" controls access to (1) information that is (2) housed in a memory, where (3) the physical address of that memory is indicated as read or write disabled, the Examiner has failed to establish a prima facie case of anticipation.

For at least the foregoing reasons, claim 7 (and the other claims in the section) is allowable.

D. Claims 5, 10, 14, 18, and 22 are patentable over *Nozue* and in view of *Childs*

Claims 5, 10, 14, 18, and 22 are allowable for at least the reasons their respective independent claims are allowable (as discussed above). These claims are further allowable for the additional features recited in the claims.

Claims 5, 10, 14, 18, and 22 specify that the "selected information" (referenced in the independent claims) is at least one of interrupt descriptor table, global descriptor table, and local descriptor table. Acknowledging that Nozue does not even "mention" these various descriptor tables, the Examiner turns to Childs and asserts that it describes protecting the table(s) at col. 4, lines 17-24. The Examiner then proceeds to provide reasons from Childs as to the benefits of protecting descriptor tables, and thereafter uses those benefits to justify why Childs is properly combinable with Nozue to arrive at the claimed invention under §103. The Examiner's approach to establishing a prima facie case of obviousness, however, is misguided. Simply reciting reasons as to why it is beneficial to protect descriptor tables in Childs is insufficient to establish a motivation to combine the two references. Rather, those reasons simply explain the motivation behind solving the problems faced by the inventors in Childs. In the instant case, to establish the requisite motivation to combine, the Examiner must show an express teaching in the references themselves that would lead one skilled in the art to extend the protection scheme of Nozue to the descriptor tables in Childs to arrive at a claimed invention that uses at least two tables (or levels) to control access to descriptor tables. Here, the Examiner has failed to do so, and, as explained below, cannot do so.

The Nozue scheme uses tables in Figures 24A and 45 for providing protection for threads and programs. In particular, the scheme seeks to protect programs from invading the logical address space of other programs (see Figure 45) and also provides a translation look-aside buffer table (in Figure 29A) to assign permission rights to threads. Naturally, because tables in Figures 24A and 45 are intended to protect threads/programs, it is not surprising that Nazue does not

even mention the use of descriptor tables and certainly does not suggest extending the Figure 24A/Figure 45 tables to protect descriptor tables. In fact, the Nazue negates any motivation to combine the two references in the suggested manner. For example, Figure 24A of Nazue is directed to a translation look-aside buffer (which translates logical addresses to physical addresses). Incorporating the descriptor tables of Childs in such a translation look-aside buffer for additional protection would be nonsensical. Similarly, it would make be nonsensical to extend Nozue's program management table (Figure 45), a table that manages programs, to protect descriptor tables of Childs, even though that is precisely what the Examiner's suggests. Thus, notwithstanding the Examiner's assertion, Nazue fails to provide any motivation or suggestion for combining the references in the manner suggested to arrive at the claimed invention (use of two tables or levels to protect the descriptor tables).

Like Nozue, Childs also fails to provide the requisite motivation or suggestion to combine. Childs, while it describes protecting descriptor tables, it does not describe protecting them using multiple tables or levels (as the claims call for). To the contrary, Childs describes protecting descriptor tables through the use of a selector, which comprises an index integer assigned to the descriptor at the time of its creation. *See* Childs, 4:21-24. The Examiner fails to provide why a skilled artisan would turn away from the selector-based based scheme of Childs and would be motivated to combine it with the program management table and translation look-aside table of Nozue Thus, like Nozue, Childs fails to provide any motivation to combine the two references. For at least this reason, the Examiner has failed to establish a prima facie case of obviousness. As such, claims 5, 10, 14, 18, and 22 are allowable.

E. Claim 6 is patentable over *Nozue* and in view of *Childs*

Claims 6 is allowable for at least the reasons its independent claims is allowable (as discussed above). Additionally, claim 6 is also allowable over the cited references because it recites an additional feature not taught by Nozue and Childs. Claim 6 calls for using a stack in the computer system to verify the identity of the program. The Examiner asserts that this feature is taught in Childs at col. 9, lines 30-40. The Applicants respectfully disagree. The passage cited by the Examiner describes using a stack to adjust a privilege level field (specifically RPL field) of a selector parameter. In contrast, claim 6 calls for using a stack to verify the identity of the program requesting to access the selected information. As such, Childs fails to disclose the claimed feature. Accordingly, claim 6 is allowable.

VII. CLAIMS APPENDIX

The claims that are the subject of the present appeal are set forth in the attached Claims Appendix.

IX. EVIDENCE APPENDIX

There is no evidence relied upon in this Appeal with respect to this section.

X. RELATED PROCEEDINGS APPENDIX

There are no related appeals and/or interferences that might affect the outcome of this proceeding.

In view of the foregoing, it is respectfully submitted that the Examiner erred in not allowing all claims pending in the present application over the prior art of record. **The undersigned attorney may be contacted at (713) 934-4064** with respect to any questions, comments, or suggestions relating to this Appeal Brief.

Respectfully submitted,

WILLIAMS, MORGAN & AMERSON, P.C.
CUSTOMER NO. 23720

Date: 5/2/06

By: _____

Ruben S. Bains
Reg. No. 46,532
10333 Richmond, Suite 1100
Houston, Texas 77042
(713) 934-4064
(713) 934-7011 (facsimile)
ATTORNEY FOR APPLICANT(S)

CLAIMS APPENDIX

1. (Previously Amended) A method for providing security in a computer system, comprising:

controlling access to selected information using attributes defined in a first table;

controlling access to the selected information using a second table that associates at least one of a read and write privilege with one or more physical addresses of a memory that houses the selected information;

receiving a request from a program to access the information; and

allowing access to the information in response to determining that the program has the authority to access the information based on at least one of the read and write privilege.

2. (Previously Amended) The method of claim 1, wherein controlling access to the selected information based on the privilege comprises:

indicating in the second table that the memory housing the information is at least one of read and write disabled.

3. (Previously Amended) The method of claim 2, wherein the second table is a bitmap based on physical addresses of the memory.

4. (Original) The method of claim 1, wherein the program is an operating system.

5. (Previously Amended) The method of claim 1, wherein the selected information is at least one of interrupt descriptor table, global descriptor table, and local descriptor table.

6. (Previously Amended) The method of claim 1, wherein allowing access to the information in response to determining that the program has the authority to access the information includes using a stack in the computer system to verify the identity of the program.

7. (Original) A method for providing security, comprising:

writing to at least one register to define a privileged memory region;

defining at least one computer instruction as a privileged instruction, wherein the privileged instruction is resident in the privileged memory region;

identifying information for protection;

indicating at least one physical address of a memory that houses the information as at least one of read and write disabled; and

controlling the access to the information using the privileged instruction.

8. (Original) The method of claim 7, further including writing to a second register, wherein the first and second registers define the privileged memory region.

9. (Original) The method of claim 7, wherein indicating at least one physical address of the memory includes:

generating a table based on the physical addresses of the memory; and

indicating in the table that the memory housing the information is at least one of read and write disabled.

10. (Original) The method of claim 7, wherein the information is at least one of interrupt descriptor table, global descriptor table, and local descriptor table.

11. (Previously Amended) A computer readable program storage device encoded with instructions that, when executed by a computer, performs a method of providing security, comprising:

protecting selected information using a first level of security specifying access privileges to the selected information;

protecting the information using a second level of security that associates at least one of a read and write privilege with one or more physical addresses of a memory that houses the selected information;

receiving a request from a program to access the selected information; and

accessing the information in response to determining that the program has the authority to access the selected information based at least on the second security level.

12. (Original) The computer readable program storage device of claim 11, wherein indicating at least one physical address of the memory includes:

generating a table based on the physical addresses of the memory; and

indicating in the table that the memory housing the information is at least one of read and write disabled.

13. (Previously Amended) The computer readable program storage device of claim 12, wherein the table includes an entry specifying access rights to the selected information based on one or more programs desiring to access the selected information.

14. (Original) The computer readable program storage device of claim 11, wherein the information is at least one of interrupt descriptor table, global descriptor table, and local descriptor table.

15. (Previously Amended) An apparatus, comprising:

a memory comprising:

a first level of protection specifying access privileges for selected information; and

a privileged code, the privileged code capable of:

protecting access to the selected information based on a second level of protection in which at least one of a read and write privilege is associated with the physical address of a memory housing the information;

receiving a request from a program to access the information; and

allowing access to the information in response to determining that the program has the authority to access the information based on at least one of the read and write privilege.

16. (Original) The apparatus of claim 15, wherein the privileged code capable of indicating at least one physical address of the memory includes the privileged code being capable of:

generating a table based on the physical addresses of the memory; and

indicating in the table that the memory housing the information is at least one of read and write disabled.

17. (Original) The apparatus of claim 15, wherein the program is an operating system.

18. (Original) The apparatus of claim 15, wherein the information is at least one of interrupt descriptor table, global descriptor table, and local descriptor table.

19. (Previously Amended) A system, comprising:

a processor; and

a memory coupled to the processor, the memory comprising:

a table specifying access privileges for selected information; and

a privileged code capable of:

protecting access to the selected information based a second table specifying association of at least one of a read and write privilege with at least one physical address of a memory housing the information;

receiving a request from a program to access the information; and

allowing access to the information in response to determining that the program has the authority to access the information based on at least one of the read and write privilege.

20. (Original) The system of claim 19, wherein the privileged code capable of indicating at least one physical address of the memory includes the privileged code being capable of:

generating a table based on the physical addresses of the memory; and

indicating in the table that the memory housing the information is at least one of read and write disabled.

21. (Original) The system of claim 19, wherein the program is an operating system.

22. (Original) The system of claim 19, wherein the information is at least one of interrupt descriptor table, global descriptor table, and local descriptor table.

23. (Original) The system of claim 19, wherein the processor is an x86 processor.

24. (Previously Amended) An apparatus for providing security, comprising:

means for providing a first table of at least write protection for selected information;

means for providing a second table of at least one of read and write protection for the selected information associated with one or more physical addresses of a memory that houses the selected information;

means for receiving a request from a program to access the information; and

means for allowing access to the information in response to determining that the program has the authority to access the information based on at least the first and second tables.